UNITED STATES DISTRICT COURT

for the
District of South Dakota

In the Matter of the Search of: The properties located at [redacted] Hot Springs, SD 57747, and to search any curtilage and outbuildings, as well as persons or vehicles on the property as well as the content of any computer and electronic storage devices	)	Case No. 5:20-mj-195 **REDACTED**

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location):*

SEE "ATTACHMENT A, C, D", which is attached to and incorporated in this Application and Affidavit

located in the District of South Dakota, there is now concealed *(identify the person or describe the property to be seized)*:

SEE "ATTACHMENT B", which is attached to and incorporated in this Application and Affidavit

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☒ evidence of a crime;
- ☒ contraband, fruits of crime, or other items illegally possessed;
- ☒ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
18 U.S.C. §§ 2251, 2252, 2252A	Production, distribution, receipt and possession of child pornography

The application is based on these facts:

☒ Continued on the attached affidavit, which is incorporated by reference.

☐ Delayed notice of ____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

☐ Your applicant requests that no notice be given prior to the execution of the search warrant, i.e., "no knock", the basis of which is set forth in the attached affidavit.

☐ Your applicant requests authorization to serve the search warrant any time day or night pursuant to Fed. R. Crim. P. 41(e)(2)(A)(ii), the basis of which is set forth in the attached affidavit.

Applicant's signature

Sarah B. Collins, AUSA
Printed name and title

Sworn to before me and: ☐ signed in my presence.
☒ submitted, attested to, and acknowledged by reliable electronic means.

Date: 9/11/20

Judge's signature

City and state: Rapid City, SD

Daneta Wollmann, U.S. Magistrate
Printed name and title

UNITED STATES DISTRICT COURT
DISTRICT OF SOUTH DAKOTA
WESTERN DIVISION

IN THE MATTER OF THE SEARCH OF:
The properties located at [redacted] Hot Springs, SD 57747, and to search any curtilage and outbuildings, as well as persons or vehicles on the property as well as the content of any computer and electronic storage devices

CASE NUMBER: 5:20-mj-195

AFFIDAVIT IN SUPPORT OF SEARCH WARRANT APPLICATION

REDACTED

State of South Dakota)
) ss
County of Pennington)

I, Jesse Fagerland, Investigator with the Criminal Investigation Division at the Pennington County Sheriff's Office, being duly sworn, states as follows:

1. I am a certified Law Enforcement Officer through the South Dakota Law Enforcement Academy and have over 1,500 hours of formal and informal training. I began my law enforcement career in January 2008 with the Pennington County Sheriff's Office in the Patrol Division. I have served in several different capacities within the Sheriff's Office, including Patrol, Warrants, Transports, and School Resource Deputy. In May 2017, I was selected to work in the Criminal Investigation Division as an Investigator. I have received specialized training in Investigative Interviewing. During my tenure as an investigator, I have been assigned and investigated cases including assaults, rapes, and death investigations. In January, 2019, I was assigned to the Unified Narcotics Enforcement Team (UNET) Drug Task Force as an Investigator. In March, 2020, I was assigned to my current position as an Investigator with the

Internet Crimes Against Children (ICAC) Task Force. The investigations worked by this unit include child pornography, solicitation of minors, sexual exploitation of minors, disseminating harmful materials to minors, and human trafficking. Due to the placement on the task force, I have also been given the title of Special Assistant Attorney General of the State of South Dakota.

2. During my law enforcement career, I have become familiar with the *modus operandi* of persons involved in attempted production of child pornography in violation of federal law. Based on my experience and training, I am knowledgeable of the various means utilized by individuals who illegally attempt to cause minors to produce images of child pornography.

3. The information set forth below is based upon my knowledge of an investigation conducted by the South Dakota Internet Crimes Against Children Taskforce (ICAC) and the investigation of other law enforcement agents and officers including, but not limited to, South Dakota Division of Criminal Investigation (DCI), Homeland Security Investigations (HSI), the Rapid City Police Department, and the Pennington County Sheriff's Office. I have not included every fact obtained pursuant to this investigation, but have set forth those facts that I believe are essential to establish the necessary probable cause for the criminal complaint. I have not omitted any material fact relevant to the consideration of probable cause for a criminal complaint against the above named defendant.

4. I have investigated and assisted in the investigation of cases involving the possession, receipt, and distribution of child pornography in

violation of federal law to include United States Statues 18 U.S.C. §§ 2251, 2252 and 2252A. During my law enforcement-career, I have become familiar with the *modus operandi* of persons involved in the illegal production, distribution and possession of child pornography and those who engage in enticement of minors using the internet. Based on my experience and training, I am knowledgeable of the various means utilized by individuals who illegally produce, distribute, receive and possess child pornography.

5. I have been informed that 18 U.S.C. §§ 2251, 2252 and 2252A, prohibit the production, distribution, receipt and possession of child pornography.

6. Your affiant respectfully submits that there is probable cause to believe that Brian Lynn Spitzer committed the crime of attempted production of child pornography and that evidence of that crime is present in his home and office, particularly in the devices located therein.

ITEMS TO BE SEARCHED FOR AND SEIZED:

7. The properties located at [redacted] Hot Springs, SD 57747. The properties further described as a tan in color single-family house with a darker color garage, there are two separate metal buildings, grey in color with darker grey trim and white garage doors (also referred to in the affidavit as SUBJECT PREMISES and photographically depicted in Attachments C and D). I also request the warrant include authorization to search any curtilage on the property, persons on the property, outbuildings, including but not limited to the two grey metal buildings described above, detached garages

and storage sheds, as well as persons or vehicles. Additionally, your affiant seeks the warrant authorize the search the content of any computer and electronic storage devices, cellular phones, tablets, and any other electronic storage devices, including but not limited to external and internal hard drives, thumb drives, flash drives, gaming devices with storage capability, storage discs, SD cards, cameras, cellular phones, smart phones and phones with photo-taking and/or internet access capabilities. I respectfully request the Court permit law enforcement to seize all such electronic devices located on the premises and further access and search the contents of said electronic devices without seeking an additional or separate warrant.

8. The warrant is being obtained in order to search for contraband and evidence, fruits, and instrumentalities of violations of 18 U.S.C. §§ 2251, 2252 and 2252A (production, distribution, receipt and possession of child pornography) and which items are more specifically described in Attachment B.

DEFINITIONS

9. The following definitions apply to this Affidavit and Attachments A and B:

a. "Chat," as used herein, refers to any kind of text communication over the Internet that is transmitted in real-time from sender to receiver. Chat messages are generally short in order to enable other participants to respond quickly and in a format that resembles an oral conversation. This feature distinguishes chatting from other text-based online communications such as Internet forums and email.

b. "Child Erotica," as used herein, means materials or items that are sexually arousing to persons having a sexual interest in minors but that are not necessarily, in and of themselves, obscene or that do not necessarily depict minors in sexually explicit poses or positions.

c. "Child pornography," as defined in 18 U.S.C. § 2256(8), is any visual depiction of sexually explicit conduct where (a) the production of the visual depiction involved the use of a minor engaged in sexually explicit conduct, (b) the visual depiction is a digital image, computer image, or computer-generated image that is, or is indistinguishable from, that of a minor engaged in sexually explicit conduct, or (c) the visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaged in sexually explicit conduct.

d. "Cloud-based storage service," as used herein, refers to a publically accessible, online storage provider that collectors of child pornography can use to store and trade child pornography in larger volumes. Users of such a service can share links and associated passwords to their stored files with other traders of child pornography in order to grant access to their collections. Such services allow individuals to easily access these files through a wide variety of electronic devices such as desktop and laptop computers, mobile phones, and tablets, anywhere and at any time. An individual with the password to file stored on a cloud-based service does not need to be a user of the service to access the file. Access is free and readily available to anyone who has an internet connection.

e. "Computer," as used herein, refers to "an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device" and includes smartphones, and mobile phones and devices. See 18 U.S.C. § 1030(e)(1).

f. "Computer hardware," as used herein, consists of all equipment which can receive, capture, collect, analyze, create, display, convert, store, conceal, or transmit electronic, magnetic, or similar computer impulses or data. Computer hardware includes any data-processing devices (including, but not limited to, central processing units, internal and peripheral storage devices such as fixed disks, external hard drives, floppy disk drives and diskettes, and other memory storage devices); peripheral input/output devices (including, but not limited to, keyboards, printers, video display monitors, and related communications devices such as cables and connections), as well as any devices, mechanisms, or parts that can be used to restrict access to computer hardware (including, but not limited to, physical keys and locks).

g. "Computer software," as used herein, is digital information which can be interpreted by a computer and any of its related components to direct the way they work. Computer software is stored in electronic, magnetic, or other digital form. It commonly includes programs to run operating systems, applications, and utilities.

h. "Computer-related documentation," as used herein, consists of written, recorded, printed, or electronically stored material which explains or illustrates how to configure or use computer hardware, computer software, or other related items.

i. "Computer passwords, pass-phrases and data security devices," as used herein, consist of information or items designed to restrict access to or hide computer software, documentation, or data. Data security devices may consist of hardware, software, or other programming code. A password or pass-phrase (a string of alpha-numeric characters) usually operates as a sort of digital key to "unlock" particular data security devices. Data security hardware may include encryption devices, chips, and circuit boards. Data security software of digital code may include programming code that creates "test" keys or "hot" keys, which perform certain pre-set security functions when touched. Data security software or code may also encrypt, compress, hide, or "booby-trap" protected data to make it inaccessible or unusable, as well as reverse the progress to restore it.

j. A provider of "Electronic Communication Service" ("ESP"), as defined in 18 U.S.C. § 2510(15), is any service that provides to users thereof the ability to send or receive wire or electronic communications. For example, "telephone companies and electronic mail companies" generally act as providers of electronic communication services. *See* S. Rep. No. 99-541 (1986), reprinted in 1986 U.S.C.C.A.N. 3555, 3568.

k. "Electronic Storage Device" includes but is not limited to external and internal hard drives, thumb drives, flash drives, SD cards, gaming devices with storage capability, storage discs (CDs and DVDs), cameras, cellular phones, smart phones and phones with photo-taking and/or internet access capabilities, and any "cloud" storage by any provider.

l. "File Transfer Protocol" ("FTP"), as used herein, is a standard network protocol used to transfer computer files from one host to another over a computer network, such as the Internet. FTP is built on client-server architecture and uses separate control and data connections between the client and the server.

m. "Hash value," as used herein, refers to a unique alpha-numeric identifier for a digital file. A hash value is generated by a mathematical algorithm, based on the file's content. A hash value is a file's "digital fingerprint." Two files having identical content will have the same hash value, even if the file names are different. On the other hand, any change to the data in a file, however slight, will change the file's hash value, even if the file name is unchanged. Thus, if two files have the same hash value, they are said to be identical, even if they have different file names.

n. "Internet Protocol address" or "IP address," as used herein, refers to a unique number used by a computer or other digital device to access the Internet. An IP address is one of two versions. Internet Protocol Version 4 (IPV4) or Internet Protocol Version 6 (IPV6). IPV4 looks like a series of four numbers, each in the range 1-255, separated by periods. IPV6 looks like a series

of 8 numbers or letters separated by a colon. Each series of numbers will be 0-9 and/or a-f. Every computer or device accessing the Internet must be assigned an IP address so that Internet traffic sent from and directed to that computer or device may be properly directed from its source to its destination. Most Internet Service Providers (ISPs – defined below) control a range of OP addresses. IP addresses can be "dynamic," meaning that the ISP assigns a different unique number to a computer every time it accesses the Internet. IP addresses might also be "static," if an ISP assigns a user's computer a particular IP address that is used each time the computer accesses the Internet. ISPs

o. "Internet Service Providers" ("ISPs"), as used herein, are commercial organizations that are in business to provide individuals and businesses access to the Internet. ISPs provide a range of functions for their customers including access to the Internet, web hosting, e-mail, remote storage, and co-location of computers and other communications equipment.

p. "Records," "documents," and "materials," as used herein, include all information recorded in any form, visual or aural, and by any means, whether in handmade, photographic, mechanical, electrical, electronic, or magnetic form.

q. "Remote Computing Service" ("RCS"), as defined in 18 U.S.C. § 2711(2), is the provision to the public of computer storage or processing services by means of an electronic communications system.

r. "Short Message Service" ("SMS"), as used herein, is a service used to send text messages to mobile phones. SMS is also often referred to as

texting, sending text messages or text messaging. The service allows for short text messages to be sent from one cell phone to another cell phone or from the Web to another cell phone. The term "computer," as defined in 18 U.S.C. § 1030(e)(1), means an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical, arithmetic, or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device.

BACKGROUND ON CHILD PORNOGRAPHY, COMPUTERS, THE INTERNET, AND EMAIL

10. I have had both training and experience in the investigation of computer-related crimes. Based on my training, experience, and knowledge, I know the following:

a. Computers and digital technology have dramatically changed the way in which individuals interested in child pornography interact with each other. Computers basically serve four functions in connection with child pornography: production, communication, distribution, and storage.

b. Child pornographers can now transfer printed photographs into a computer-readable format with a device known as a scanner. Furthermore, with the advent of digital cameras and smartphones with cameras, when the photograph is taken it is saved as a digital file that can be directly transferred to a computer by simply connecting the camera or smartphone to the computer. In the last ten years, the resolution of pictures taken by digital cameras and smartphones has increased dramatically, meaning that such

pictures have become sharper and crisper. Photos taken on a digital camera or smartphone may be stored on a removable memory card in the camera or smartphone. These memory cards often store up to 32 gigabytes of data, which provides enough space to store thousands of high-resolution photographs. Video camcorders, which once recorded video onto tapes or mini-CDs, now can save video footage in a digital format directly to a hard drive in the camera. The video files can be easily transferred from the camcorder to a computer.

c. A device known as a modem allows any computer to connect to another computer through the use of telephone, cable, or wireless connection. Electronic contact can be made to literally millions of computers around the world. The ability to produce child pornography easily, reproduce it inexpensively, and market it anonymously (through electronic communications) has drastically changed the method of distribution and receipt of child pornography. Child pornography can be transferred via electronic mail or through file transfer protocols (FTPs) to anyone with access to a computer and modem. Because of the proliferation of commercial services that provide electronic mail service, chat services (i.e., "Instant Messaging"), and easy access to the Internet, the computer is a preferred method of distribution and receipt of child pornographic materials.

d. The computer's ability to store images in digital form makes the computer itself an ideal repository for child pornography. The size of the electronic storage media (commonly referred to as the hard drive) used in home computers has grown tremendously within the last several years. These drives

can store thousands of images at very high resolution. In addition, there are numerous options available for the storage of computer or digital files. One-Terabyte external and internal hard drives are not uncommon. Other media storage devices include CDs, DVDs, and "thumb," "jump," or "flash" drives, which are very small devices which are plugged into a port on the computer. It is extremely easy for an individual to take a photo or a video with a digital camera or camera-bearing smartphone, upload that photo or video to a computer, and then copy it (or any other files on the computer) to any one of those media storage devices (CDs and DVDs are unique in that special software must be used to save or "burn" files onto them). Media storage devices can easily be concealed and carried on an individual's person. Smartphones and/or mobile phones are also often carried on an individual's person.

e. The Internet affords individuals several different venues for obtaining, viewing, and trading child pornography in a relatively secure and anonymous fashion.

f. Individuals also use online resources to retrieve and store child pornography, including services offered by Internet Portals such as Yahoo! and Hotmail, among others. The online services allow a user to set up an account with a remote computing service that provides e-mail services as well as electronic storage of computer files in any variety of formats. A user can set up an online storage account from any computer with access to the Internet. Even in cases where online storage is used, however, evidence of child pornography can be found on the user's computer or external media in most cases.

g. As is the case with most digital technology, communications by way of computer can be saved or stored on the computer used for these purposes. Storing this information can be intentional, i.e., by saving an e-mail as a file on the computer or saving the location of one's favorite websites in, for example, "bookmarked" files. Digital information can also be retained unintentionally, e.g., traces of the path of an electronic communication may be automatically stored in many places (e.g., temporary files or ISP client software, among others). In addition to electronic communications, a computer user's Internet activities generally leave traces or "footprints" in the web cache and history files of the browser used. Such information is often maintained indefinitely until overwritten by other data.

SPECIFICS OF SEARCH AND SEIZURE OF COMPUTER SYSTEMS

11. Based upon my training and experience and information related to me by agents and others involved in the forensic examination of computers, I know that computer data can be stored on a variety of systems and storage devices including hard disk drives, floppy disks, compact disks, magnetic tapes and memory chips. I also know that during the search of the premises it is not always possible to search computer equipment and storage devices for data for a number of reasons, including the following:

a. Searching computer systems is a highly technical process which requires specific expertise and specialized equipment. There are so many types of computer hardware and software in use today that it is impossible to bring to the search site all of the technical manuals and specialized equipment

necessary to conduct a thorough search. In addition, it may also be necessary to consult with computer personnel who have specific expertise in the type of computer, software application or operating system that is being searched;

b. Searching computer systems requires the use of precise, scientific procedures which are designed to maintain the integrity of the evidence and to recover "hidden," erased, compressed, encrypted or password-protected data. Computer hardware and storage devices may contain "booby traps" that destroy or alter data if certain procedures are not scrupulously followed. Since computer data is particularly vulnerable to inadvertent or intentional modification or destruction, a controlled environment, such as a law enforcement laboratory, is essential to conducting a complete and accurate analysis of the equipment and storage devices from which the data will be extracted;

c. The volume of data stored on many computer systems and storage devices will typically be so large that it will be highly impractical to search for data during the execution of the physical search of the premises; and

d. Computer users can attempt to conceal data within computer equipment and storage devices through a number of methods, including the use of innocuous or misleading filenames and extensions. For example, files with the extension ".jpg" often are image files; however, a user can easily change the extension to ".txt" to conceal the image and make it appear that the file contains text. Computer users can also attempt to conceal data by using encryption, which means that a password or device, such as a "dongle" or "keycard," is

necessary to decrypt the data into readable form. In addition, computer users can conceal data within another seemingly unrelated and innocuous file in a process called "steganography." For example, by using steganography a computer user can conceal text in an image file which cannot be viewed when the image file is opened. Therefore, a substantial amount of time is necessary to extract and sort through data that is concealed or encrypted to determine whether it is evidence, contraband or instrumentalities of a crime.

12. Based on my own experience and my consultation with other agents who have been involved in computer searches, searching computerized information for evidence or instrumentalities of a crime often requires the seizure of all of a computer system's input and output peripheral devices, related software, documentation, and data security devices (including passwords) so that a qualified computer expert can accurately retrieve the system's data in a laboratory or other controlled environment. There are several reasons that compel this conclusion:

a. The peripheral devices that allow users to enter or retrieve data from the storage devices vary widely in their compatibility with other hardware and software. Many system storage devices require particular input/output devices in order to read the data on the system. It is important that the analyst be able to properly re-configure the system as it now operates in order to accurately retrieve the evidence listed above. In addition, the analyst needs the relevant system software (operating systems, interfaces, and hardware drivers) and any applications software which may have been used to create the

data (whether stored on hard drives or on external media), as well as all related instruction manuals or other documentation and data security devices; and

b. In order to fully retrieve data from a computer system, the analyst also needs all magnetic storage devices, as well as the central processing unit (CPU). In cases like the instant one where the evidence consists partly of image files, the monitor and printer are also essential to show the nature and quality of the graphic images which the system could produce. Further, the analyst again needs all the system software (operating systems or interfaces, and hardware drivers) and any applications software which may have been used to create the data (whether stored on hard drives or on external media) for proper data retrieval.

13. Additionally, based upon my training and experience and information related to me by agents and others involved in the forensic examination of computers, I know that routers, modems, and network equipment used to connect computers to the Internet often provide valuable evidence of, and are instrumentalities of, a crime. This is equally true of so-called "wireless routers," which create localized networks that allow individuals to connect to the Internet wirelessly. Though wireless networks may be "secured" (in that they require an individual to enter an alphanumeric key or password before gaining access to the network) or "unsecured" (in that an individual may access the wireless network without a key or password), wireless routers for both secured and unsecured wireless networks may yield significant evidence of, or serve as instrumentalities of, a crime—including, for example, serving as the

instrument through which the perpetrator of the Internet-based crime connected to the Internet and, potentially, containing logging information regarding the time and date of a perpetrator's network activity as well as identifying information for the specific device(s) the perpetrator used to access the network. Moreover, I know that individuals who have set up either a secured or unsecured wireless network in their residence are often among the primary users of that wireless network.

PROBABLE CAUSE AND BACKGROUND OF THE INVESTIGATION

14. In August 2020, South Dakota ICAC and Homeland Security Investigations collaborated to conduct an online operation targeting internet child predators using various websites and applications utilized for strangers to meet. On August 9, 2020, Homeland Security Investigations Special Agent Richie Berger posted "BF Cheated on me...Mad AF....Any ideas" on Craigslist. Craigslist user "62c2," later identified as Brian Lynn Spitzer, replied, "Revenge fuck". Throughout the rest of the conversation via Craigslist the following is a summary of the information exchanged:

- 62c2 asks for age and picture of the person who posted on Craigslist.
- SA Berger tells 62c2 they are 15 years old.
- 62c2 states they were not anticipating the Craigslist poster to be so young and then asked for a picture two additional times.
- 62c2 reiterates "a good fucking by another guy should help".
- SA Berger sends a picture of a girl who appears to be approximately 15 years of age
- 62c2 states, "Damn cute. So your 15... what age your first time? With this POS ex?"
- 62c2 states they are 56 years old and have "a lot of experiences to share".
- When SA Berger responds, "That would be fun. I'm curious", 62c2 responds, "Not what I expected to hear for sure... most go no fucking way .... your old enough to be my gpa lol".

- 62c2 wants to know if the Craigslist poster "got revenge fucked" and provides the poster with a phone number to text message them at: 891-3053 (the messages continue on text messages for the duration of the conversation).
- The phone number was identified by HSI Criminal Analyst Amber Cooper to belong to Spitzer Construction Inc. Per Verizon records, the phone should be a SAMSUNG GALAXY NOTE10 PL BLK 256.
- Spitzer states his name is "Brian" while SA Berger states his name is "Christy".
- SA Berger again states Christy is 15 years old.
- Spitzer continues to be interested in Christy's sex life by asking her questions about it.
- Spitzer states, "I also have a kink for younger women".
- Spitzer entertains the idea of meeting with Christy but ultimately decides he only has one hour to spare and that is not enough time to meet up.
- Spitzer continues to engage in sexual conversation with Christy.
- Spitzer states, "See I'm being careful.... your underage".

15. Spitzer's communication with SA Berger started on August 9, 2020 and ended on August 10, 2020. Their communication moved to text message and went from August 10, 2020 to August 12, 2020, when the following communication occurred:

- SA Berger: its funny you were here and didn't text when you were. i think youre just like most other older men and just want to fanatasize and play with youerself
- Spitzer: I don't have time for juvenile attitude.... Good bye
- SA Berger: I don't have time for a creepy married man trying to have sex with me while his wife is in an MRI machine.

16. SSA Brent Gromer elected not to pursue charges on Spitzer at that time, but rather after the operation ended, using a different persona, give Spitzer another opportunity to attempt to entice a minor to engage in unlawful sex using the internet.

17. On August 24, 2020, utilizing my Callyo phone number (320-208-9936), I sent a text to 605-891-3053, Spitzer's number stating my name is Jenna

and I am Christy's friend. The following is a summary of my conversation with Spitzer:

August 24th

- Spitzer stated he couldn't remember who Christy was but stated he remembered when I told him she was the 15 year old girl he had been chatting with.
- Spitzer asked Jenna's age; I responded by telling him 14.
- Spitzer asked to see Jenna's "angel face"; I replied with a photo of a Law Enforcement Officer taken of her when she was 14 years old.
- Spitzer replied to the photo, "Yup angelic" and "Well your a very cute young lady".
- I asked Spitzer for a photo; he complied and stated, "Just now while driving"
- Spitzer asked several questions regarding Jenna's sex life to include if a guy has licked her "pussy", "missionary" position, "doggy" position, "cowgirl" position, "reverse cowgirl" position and "rimming" (described by Spitzer as "...I lick your tiny ass..."
- While talking about sexual topics, Spitzer stated, "I prefer younger".
- Spitzer stated the youngest person he had sex with as an adult was 23 but clarified he had sex with a 13 year old when he was 14.
- I asked Spitzer if 14 was too young for him, he replied, "What do you think". I responded that I didn't know; he replied, "Not". I clarified, "not too young???"; he responded , "no".
- Spitzer then began questioning Jenna again on her sex life.
- When asked if Jenna was on birth control, I responded, "no..."she (referring to her mother) has no idea im fucking..."she still thinks im just a little girl"; Spitzer responded, "So your risking it sometimes..."Well you are!"..."Innocent and all".
- Spitzer stated, "A tad horny now aren't you"; I replied, "why would you say that?"; Spitzer replied, "I know 14 year olds", and continued to talk sexually to Jenna.

August 25th

- Spitzer stated he lives in Hot Springs and owns his own contracting business.
- I stated it's hard for a 14 year old to earn money; Spitzer replied, "Oh you'll do that soon enough... remember in the meantime be 14! Have fun!"..."There's a few things you can do that come to mind". When asked what, Spitzer replied, "Be a sugar baby". Spitzer explained what a "sugar baby" was by stating, "Taking care of a man that takes care of you. Basically don't give the pussy away for free". When I told him I've been a "sugar baby" in the past, Spitzer replied, "Good

girl". Spitzer continued to encourage Jenna to get paid in exchange for sexual favors and stated, "Many do though so insist on it... your prime at your age... only 14 once".
- Spitzer questioned Jenna on what kind of "panties" she wears. Spitzer stated, "I like panties on the floor or in the drawer... you should go commando". I replied by telling Spitzer I would wear no panties the following day; Spitzer replied, "You do that! And send me proof". I responded, "Like a pic!?!"; Spitzer stated, "Duh lol".
- Spitzer stated he will start referring to Jenna as "PJ", short for "Princess Jenna"; he requested Jenna refer to him as "Big Dog".

August 26th
- Spitzer continued asking sexual questions including asking about Jenna's underwear, bra size, if Jenna is interested in a sexual relationship with "Christy" and another guy.
- Spitzer stated Jenna is "Sexy as fuck".
- Spitzer asked, "You know why I prefer mini skirts and no panties?"..."Easy to flip over your booty when i bend you over"..."And see your cute butt".
- Spitzer stated, "Mmmm perky lil tits".
- Spitzer talked about meeting up with Jenna.
- After chatting about wearing no underwear with a mini skirt on, Spitzer stated, "Mmmm don't dry that 14 year old pussy out though".

August 31st
- Spitzer asked where Jenna lived. I told him near Stevens High School. Spitzer explained the reason he asked was if there was enough time to meet up.
- I asked Spitzer what we would do if we met up, he replied, "With a beautiful young lady scantily clad with me I doubt I could keep my hands to myself".
- Spitzer stated he planned to give Jenna money so she could buy a mini skirt. He further stated, "Anything you wear will be quite cock hardening".
- Spitzer asked Jenna again what sexual positions she had tried in the past...he asked specifically if she participated in any "oral" sex.
- Spitzer sent Jenna additional pictures of himself and his property
- Spitzer again asked about where he and Jenna could meet up in the future.
- Spitzer stated, "I wish I lived within walking distance of you"..."You could go for walks anytime"..."And come visit"..."Daily fucking".
- Spitzer stated he wanted to perform anal sex on Jenna. He told her he would provide her with a "butt plug to use in between visits to keep it (Jenna's anus) trained". Spitzer further directed Jenna to use her fingers to stretch her anus out prior to their first meeting.
- Spitzer stated he would like to meet with Jenna on a weekly basis.

- When ending the conversation, Spitzer stated, "Good night princess.... finger your ass tonight a bit".

September 1

- Spitzer asked my undercover persona what "she" was wearing. After "she" told him a sundress he said he was "commando" and "cock hardening."
- During the communications, Spitzer indicated he was working at the time in his office in a shop near his house and sent a photography depicting a desk and computer.
- He asked Jenna for a massage with a "happy ending" and explained that it meant to "cum" or "climax."
- Spitzer asked Jenna how the "ass fingering went" and said that she needed the "proper arousal from" him. He then describes a "fantasy" regarding her sundress, where he would "bend" her "over" and "pull up" her "dress over" her "ass" and he would watch her "arch" her "ass up and go on tip toes" to "meet his cock." He then added he "liked" the "tipy toe thing" because it was "like pussy begging for cock."
- Again Spitzer wrote of meeting with Jenna to engage in sex.

September 2

- Spitzer tells Jenna he "has something she could rub" and that it would "grow" in her hand and that his penis is "7 inches" and she was "gunna love it."
- Jenna responded saying that was "huge" and he replied that she maybe needed to "grow up a bit" and "wait a few years to ride on the adult cock," and that she "needed to grow up someday anyway" and that "training by men does that anyway."
- Spitzer than discussing meeting again but then says she is "14" and he does not know whether she is a "cop or not" and that she "won't send pics" and added that was a "red flag" to him and it is not "worth getting in trouble for."
- When reminded by Jenna that she did send pics, Spitzer replied that they were not "in the moment" pictures. Jenna sent a picture of the person associated with law enforcement depicted in prior photos wearing a dress. He replied that she had a "great ass."
- They discussed Jenna getting in trouble for taking the picture and Jenna voiced concerns about getting her phone taken away. He gives her advice on lies to tell her mother and mentioned that "Christy," SA Berger's undercover persona, got mad at him for "asking questions."
- Spitzer then wrote that Jenna was a "sexy 14 year old."
- He then asked when she typically has her period and if she'd ever been "fucked" while having it.

18. In addition, in later conversations, Spitzer promised to buy Jenna a cellular phone in which her mother would not have access. When I asked what Jenna would have to do to get the phone he replied "learn to take 7." Jenna then wrote "what???" and Spitzer replied "inches," referring to his penis.

19. On September 7, 2020, I went to view Spitzer's Hot Springs home and office. It was difficult to conduct surveillance undetected due to its location behind a hill. I was able to see the tan house and two grey outbuildings as well as a sign that said "Spitzer Construction" and phone number 891-3053. From what I could observe, the buildings appeared to match those he sent to Jenna during their conversations.

20. CHARACTERISTICS COMMON TO INDIVIDUALS WHO HAVE A SEXUAL INTEREST IN CHILDREN AND/OR WHO PRODUCE, RECEIVE AND/OR POSSESS CHILD PORNOGRAPHY

21. Based on my previous investigative experience related to child exploitation investigations, and the training and experience of other law enforcement officers with whom I have had discussions, I know there are certain characteristics common to individuals who have a sexual interest in children and/or receive, or possess images of child pornography:

a. Individuals who have a sexual interest in children and/or receive, or possess images of child pornography may receive sexual gratification, stimulation, and satisfaction from contact with children, or from fantasies they may have viewing children engaged in sexual activity or in sexually suggestive poses, such as in person, in photographs, or other visual media, or from literature describing such activity.

b. Individuals who have a sexual interest in children and/or receive, or possess images of child pornography may collect sexually explicit or suggestive materials, in a variety of media, including photographs, magazines, motion pictures, videotapes, books, slides and/or drawings or other visual media. Individuals who have a sexual interest in children or images of children oftentimes use these materials for their own sexual arousal and gratification. Further, they may use these materials to lower the inhibitions of children they are attempting to seduce, to arouse the selected child partner, or to demonstrate the desired sexual acts.

c. Individuals who have a sexual interest in children and/or receive, or possess images of child pornography almost always possess and maintain their hard copies of child pornographic material, that is, their pictures, films, video tapes, magazines, negatives, photographs, correspondence, mailing lists, books, tape recordings, etc., in the privacy and security of their home or some other secure location. Individuals who have a sexual interest in children or images of children often retain pictures, films, photographs, negatives, magazines, correspondence, books, tape recordings, mailing lists, child erotica, and videotapes for many years.

d. Likewise, individuals who have a sexual interest in children and/or receive, or possess images of child pornography often maintain their child pornography images in a digital or electronic format in a safe, secure and private environment, such as a computer and surrounding area. These child pornography images are often maintained for several years and are kept close

by, usually at the possessor's residence, inside the possessor's vehicle, or, at times, on their person, to enable the individual to view the child pornography images, which are valued highly.

e. Individuals who have a sexual interest in children and/or receive, or possess images of child pornography also may correspond with and/or meet others to share information and materials, rarely destroy correspondence from other child pornography distributors/possessors, conceal such correspondence as they do their sexually explicit material, and often maintain lists of names, addresses, and telephone numbers of individuals with whom they have been in contact and who share the same interests in child pornography.

f. Individuals who have a sexual interest in children and/or receive, or possess images of child pornography prefer not to be without their child pornography for any prolonged time period. This behavior has been documented by law enforcement officers involved in the investigation of child pornography throughout the world. Thus, even if Brian Lynn Spitzer or another person in the house uses a portable device (such as a mobile cell phone) to access the internet and child pornography, it is more likely than not that evidence of this access will be found in his home, the SUBJECT PREMISES, as well as on electronic devices found in the home, as previously detailed and as set forth in Attachment A.

REQUEST FOR SEALING OF APPLICATION/AFFIDAVIT

22. I request that the Court order that all papers submitted in support of this application, including this affidavit, the application, the warrant, and the Order itself, be sealed until further order of the Court. These documents discuss an ongoing criminal investigation that is neither public nor known to all the targets of the investigation. Accordingly, there is good cause to seal these documents because their premature disclosure may give targets an opportunity to flee, destroy or tamper with evidence, change patterns of behavior, notify confederates, or otherwise seriously jeopardize the investigation.

CONCLUSION

23. Based on my training and experience, and the facts as set forth in this affidavit, there is probable cause to believe that there exists evidence of a crime, contraband, instrumentalities, and/or fruits of violations of criminal laws as specified herein, are located at the SUBJECT PREMISES, described further in Attachment A. I respectfully request that this Court issue a search warrant for the SUBJECT PREMISES, authorizing the seizure and search of the items described in Attachment B.

24. I am aware that the recovery of data by a computer forensic analyst takes significant time; much the way recovery of narcotics must later be forensically evaluated in a lab, digital evidence will also undergo a similar process. For this reason, the "return" inventory will contain a list of only the tangible items recovered from the premises. Unless otherwise ordered by the Court, the return will not include evidence later examined by a forensic analyst.

Dated: 9-11-20

Jesse Fagerland

Investigator Jesse Fagerland
Pennington County Sheriff's Office
Internet Crimes Against Children
Taskforce

SUBSCRIBED and SWORN to

_____ in my presence
_X__ by reliable electronic means

this 11th day of September, 2020.

U.S. MAGISTRATE JUDGE

ATTACHMENT A
Property to Be Searched

- The property located at [redacted] Hot Springs, SD 57747. The properties further described as a tan in color single-family house with two grey in color metal buildings (also referred to in the affidavit as SUBJECT PREMISES and photographically depicted in Attachments C and D);
- any curtilage on the property;
- persons on the property;
- outbuildings, detached garages and storage sheds;
- vehicles on the property;
- the content of any computer and electronic storage devices, cellular phones, tablets, and any other electronic storage devices, including but not limited to external and internal hard drives, thumb drives, flash drives, gaming devices with storage capability, storage discs, SD cards, cameras, smart phones and phones with photo-taking and/or internet access capabilities.

ATTACHMENT B

ITEMS TO BE SEIZED

The following materials, which constitute evidence of the commission of a criminal offense, contraband, the fruits of crime, or property designed or intended for use or which is or has been used as the means of committing a criminal offense, namely violations of Title 18, United States Code, Sections 2251, 2252 and 2252A (possession, receipt, distribution and production of child pornography):

1. Computers, cell phones or storage media used as a means to commit the violations described above.
2. For any computer or storage medium whose seizure is otherwise authorized by this warrant, and any computer or storage medium that contains or in which is stored records or information that is otherwise called for by this warrant (hereinafter, "COMPUTER"):
    a. evidence of who used, owned, or controlled the COMPUTER at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, "chat," instant messaging logs, photographs, and correspondence;
    b. evidence of software that would allow others to control the COMPUTER, such as viruses, Trojan horses, and other forms of

malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;

c. evidence of the lack of such malicious software;

d. evidence indicating how and when the computer was accessed or used to determine the chronological context of computer access, use, and events relating to crime under investigation and to the computer user;

e. evidence indicating the computer user's state of mind as it relates to the crime under investigation;

f. evidence of the attachment to the COMPUTER of other storage devices or similar containers for electronic evidence;

g. evidence of programs (and associated data) that are designed to eliminate data from the COMPUTER;

h. evidence of the times the COMPUTER was used;

i. passwords, encryption keys, and other access devices that may be necessary to access the COMPUTER;

j. documentation and manuals that may be necessary to access the COMPUTER or to conduct a forensic examination of the COMPUTER;

k. records of or information about Internet Protocol addresses used by the COMPUTER;

l. records of or information about the COMPUTER's Internet activity, including firewall logs, caches, browser history and cookies,

"bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses; and

m. contextual information necessary to understand the evidence described in this attachment.

3. Routers, modems, and network equipment used to connect computers to the Internet.

4. Child pornography and child erotica.

5. Records, information, and items relating to violations of the statutes described above including:

   a. Records, information, and items relating to the occupancy or ownership of [redacted] Hot Springs, SD 57719, including utility and telephone bills, mail envelopes, or addressed correspondence; Records, information, and items relating to the ownership or use of computer equipment found in the above residence, including sales receipts, bills for Internet access, and handwritten notes;

   b. Records and information relating to the identity or location of the persons suspected of violating the statutes described above; and

   c. Records and information relating to sexual exploitation of children, including correspondence and communications between various Seller and Buyer Accounts.

As used above, the terms "records" and "information" includes all forms of creation or storage, including any form of computer or electronic storage (such as hard disks or other media that can store data); any handmade form (such as writing); any mechanical form (such as printing or typing); and any photographic form (such as microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, or photocopies, CDs, DVDs).

The term "computer" includes all types of electronic, magnetic, optical, electrochemical, or other high speed data processing devices performing logical, arithmetic, or storage functions, including desktop computers, notebook computers, mobile phones, tablets, server computers, and network hardware.

The term "storage medium" includes any physical object upon which records computer data. Examples include external and internal hard drives, thumb drives, flash drives, gaming devices with storage capability, storage discs, SD cards, hard disks, RAM, flash memory, CDs, DVDs, and other magnetic or optical media.

ATTACHMENT C

ATTACHMENT D

UNITED STATES DISTRICT COURT

for the
District of South Dakota

In the Matter of the Search of:
The property located at [redacted] Hot Springs, SD 57747 and to search any curtilage and outbuildings, as well as persons or vehicles on the property as well as the content of any computer and electronic storage devices

Case No. 5:20-mj-195

REDACTED

SEARCH AND SEIZURE WARRANT

To: Any authorized law enforcement officer

An application by a federal law enforcement officer or an attorney for the government requests the search of the following person or property located in the District of South Dakota *(identify the person or describe the property to be searched and give its location)*:

See **ATTACHMENT A, C, D** attached hereto and incorporated by reference

I find that the affidavit, or any recorded testimony, establish probable cause to search and seize the person or property described above, and that such search will reveal *(identify the person or describe the property to be seized)*:

Evidence of a crime in violation of 18 U.S.C. §§ 2251, 2252, 2252A, as described in **ATTACHMENT B**, attached hereto and incorporated by reference.

I find that the affidavit, or any recorded testimony, establishes probable cause to search and seize the person or property.

YOU ARE COMMANDED to execute this warrant on or before September 25, 2020 *(not to exceed 14 days)*

☒ in the daytime 6:00 a.m. to 10 p.m. ☐ at any time in the day or night because good cause has been established.

Unless delayed notice is authorized below, you must give a copy of the warrant and a receipt for the property taken to the person from whom, or from whose premises, the property was taken, or leave the copy and receipt at the place where the property was taken.

The officer executing this warrant, or an officer present during the execution of the warrant, must prepare an inventory as required by law and promptly return this warrant and inventory to Daneta Wollmann.
(United States Magistrate Judge)

☐ Pursuant to 18 U.S.C. § 3103a(b), I find that immediate notification may have an adverse result listed in 18 U.S.C. § 2705 (except for delay of trial), and authorize the officer executing this warrant to delay notice to the person who, or whose property, will be searched or seized *(check the appropriate box)*
☐ for _____ days *(not to exceed 30)*. ☐ until, the facts justifying, the later specific date of _____.

☐ I find that good cause has been established to authorize the officer executing this warrant to not provide notice prior to the execution of the search warrant, i.e., "no knock".

Date and time issued: 9/11/20 at 1pm

Judge's signature

City and state: Rapid City, SD

Daneta Wollmann, U.S. Magistrate
Printed name and title

Return

Case No.: 5:20-mj-195	Date and time warrant executed:	Copy of warrant and inventory left with:

Inventory made in the presence of :

Inventory of the property taken and name of any person(s) seized:

Certification

I declare under penalty of perjury that this inventory is correct and was returned along with the original warrant to the designated judge.

Date: _____

_____
Executing officer's signature

_____
Printed name and title